

# Contents

<b>Preface</b>	<b>xiii</b>
<b>Notations</b>	<b>xv</b>
<b>1 Overview</b>	<b>1</b>
1.1 Introduction	2
1.2 Common Cryptographic Primitives	2
1.2.1 The Classical Problem: Secure Transmission of Messages	2
Symmetric-key or secret-key cryptography	4
Asymmetric-key or public-key cryptography	4
1.2.2 Key Exchange	5
1.2.3 Digital Signatures	5
1.2.4 Entity Authentication	6
1.2.5 Secret Sharing	8
1.2.6 Hashing	8
1.2.7 Certification	9
1.3 Public-key Cryptography	9
1.3.1 The Mathematical Problems	9
1.3.2 Realization of Key Pairs	10
1.3.3 Public-key Cryptanalysis	11
1.4 Some Cryptographic Terms	11
1.4.1 Models of Attacks	12
1.4.2 Models of Passive Attacks	12
1.4.3 Public Versus Private Algorithms	13
<b>2 Mathematical Concepts</b>	<b>15</b>
2.1 Introduction	16
2.2 Sets, Relations and Functions	16
2.2.1 Set Operations	17
2.2.2 Relations	17
2.2.3 Functions	18
2.2.4 The Axioms of Mathematics	19
Exercise Set 2.2	20
2.3 Groups	21
2.3.1 Definition and Basic Properties	21
2.3.2 Subgroups, Cosets and Quotient Groups	23
2.3.3 Homomorphisms	25
2.3.4 Generators and Orders	26
2.3.5 Sylow's Theorem	27
Exercise Set 2.3	29
2.4 Rings	31
2.4.1 Definition and Basic Properties	31
2.4.2 Subrings, Ideals and Quotient Rings	34
2.4.3 Homomorphisms	37
2.4.4 Factorization in Rings	39
Exercise Set 2.4	42
2.5 Integers	44

2.5.1	Divisibility . . . . .	44
2.5.2	Congruences . . . . .	45
2.5.3	Quadratic Residues . . . . .	48
2.5.4	Some Assorted Topics . . . . .	52
	The prime number theorem . . . . .	53
	Density of smooth integers . . . . .	54
	The extended Riemann hypothesis . . . . .	54
	Exercise Set 2.5 . . . . .	56
2.6	Polynomials . . . . .	57
2.6.1	Elementary Properties . . . . .	58
2.6.2	Roots of Polynomials . . . . .	59
2.6.3	Algebraic Elements and Extensions . . . . .	61
	Exercise Set 2.6 . . . . .	63
2.7	Vector Spaces and Modules . . . . .	64
2.7.1	Vector Spaces . . . . .	65
2.7.2	Modules . . . . .	69
2.7.3	Algebras . . . . .	71
	Exercise Set 2.7 . . . . .	72
2.8	Fields . . . . .	74
2.8.1	Properties of Field Extensions . . . . .	74
2.8.2	Splitting Fields and Algebraic Closure . . . . .	76
2.8.3	Elements of Galois Theory . . . . .	78
	Exercise Set 2.8 . . . . .	79
2.9	Finite Fields . . . . .	80
2.9.1	Existence and Uniqueness of Finite Fields . . . . .	80
2.9.2	Polynomials over Finite Fields . . . . .	82
2.9.3	Representation of Finite Fields . . . . .	85
	Exercise Set 2.9 . . . . .	88
2.10	Affine and Projective Curves . . . . .	90
2.10.1	Plane Curves . . . . .	90
2.10.2	Polynomial and Rational Functions on Plane Curves . . . . .	92
2.10.3	Maps Between Plane Curves . . . . .	95
2.10.4	Divisors on Plane Curves . . . . .	95
	Exercise Set 2.10 . . . . .	97
2.11	Elliptic Curves . . . . .	98
2.11.1	The Weierstrass Equation . . . . .	98
2.11.2	The Elliptic Curve Group . . . . .	101
2.11.3	Elliptic Curves over Finite Fields . . . . .	106
	Exercise Set 2.11 . . . . .	107
2.12	Hyperelliptic Curves . . . . .	111
2.12.1	The Defining Equations . . . . .	111
2.12.2	Polynomial and Rational Functions . . . . .	112
2.12.3	The Jacobian . . . . .	115
	Exercise Set 2.12 . . . . .	118
2.13	Number Fields . . . . .	119
2.13.1	Some Commutative Algebra . . . . .	120
	Ideal arithmetic . . . . .	120
	Localization . . . . .	120
	Integral dependence . . . . .	121

	Noetherian rings . . . . .	123
	Dedekind domains . . . . .	125
2.13.2	Number Fields and Rings . . . . .	125
2.13.3	Unique Factorization of Ideals . . . . .	131
2.13.4	Norms of Ideals . . . . .	135
2.13.5	Rational Primes in Number Rings . . . . .	137
2.13.6	Units in a Number Ring . . . . .	139
	Exercise Set 2.13 . . . . .	139
2.14	$p$ -adic Numbers . . . . .	143
2.14.1	The Arithmetic of $p$ -adic Numbers . . . . .	143
2.14.2	The $p$ -adic Valuation . . . . .	145
2.14.3	Hensel's Lemma . . . . .	149
	Exercise Set 2.14 . . . . .	151
2.15	Statistical Methods . . . . .	154
2.15.1	Random Variables and Their Probability Distributions . . . . .	154
2.15.2	Operations on Random Variables . . . . .	155
2.15.3	Expectation, Variance and Correlation . . . . .	159
2.15.4	Some Famous Probability Distributions . . . . .	162
	Uniform distribution . . . . .	162
	Bernoulli distribution . . . . .	163
	Normal distribution . . . . .	163
2.15.5	Sample Mean, Variation and Correlation . . . . .	164
	Exercise Set 2.15 . . . . .	165
<b>3</b>	<b>Algebraic and Number-theoretic Computations</b>	<b>173</b>
3.1	Introduction . . . . .	174
3.2	Complexity Issues . . . . .	174
3.2.1	Order Notations . . . . .	175
3.2.2	Randomized Algorithms . . . . .	177
3.2.3	Reduction Between Computational Problems . . . . .	178
	Exercise Set 3.2 . . . . .	179
3.3	Multiple-precision Integer Arithmetic . . . . .	180
3.3.1	Representation of Large Integers . . . . .	181
3.3.2	Basic Arithmetic Operations . . . . .	181
	Addition and subtraction . . . . .	182
	Multiplication . . . . .	183
	Squaring . . . . .	184
	Fast multiplication . . . . .	184
	Division . . . . .	185
	Bit-wise operations . . . . .	187
3.3.3	GCD . . . . .	187
3.3.4	Modular Arithmetic . . . . .	190
	Modular exponentiation . . . . .	190
	Montgomery exponentiation . . . . .	192
	Exercise Set 3.3 . . . . .	193
3.4	Elementary Number-theoretic Computations . . . . .	195
3.4.1	Primality Testing . . . . .	195
	Deterministic primality proving . . . . .	197
3.4.2	Generating Random Primes . . . . .	199

3.4.3	Modular Square Roots . . . . .	200
	Exercise Set 3.4 . . . . .	201
3.5	Arithmetic in Finite Fields . . . . .	204
3.5.1	Arithmetic in the Ring $\mathbb{F}_2[X]$ . . . . .	204
3.5.2	Finite Fields of Characteristic 2 . . . . .	208
3.5.3	Selecting Suitable Finite Fields . . . . .	210
3.5.4	Factoring Polynomials over Finite Fields . . . . .	212
	Square-free factorization . . . . .	212
	Distinct-degree factorization . . . . .	213
	Equal-degree factorization . . . . .	214
	Exercise Set 3.5 . . . . .	215
3.6	Arithmetic on Elliptic Curves . . . . .	218
3.6.1	Point Arithmetic . . . . .	218
3.6.2	Counting Points on Elliptic Curves . . . . .	219
	The SEA algorithm . . . . .	219
	The Satoh–FGH algorithm . . . . .	221
3.6.3	Choosing Good Elliptic Curves . . . . .	223
3.7	Arithmetic on Hyperelliptic Curves . . . . .	224
3.7.1	Arithmetic in the Jacobian . . . . .	225
3.7.2	Counting Points in Jacobians of Hyperelliptic Curves . . . . .	225
	Exercise Set 3.7 . . . . .	228
3.8	Random Numbers . . . . .	228
3.8.1	Pseudorandom Bit Generators . . . . .	228
3.8.2	Cryptographically Strong Pseudorandom Bit Generators . . . . .	229
3.8.3	Seeding Pseudorandom Bit Generators . . . . .	230
	Exercise Set 3.8 . . . . .	231
<b>4</b>	<b>The Intractable Mathematical Problems</b> . . . . .	<b>237</b>
4.1	Introduction . . . . .	238
4.2	The Problems at a Glance . . . . .	239
	Exercise Set 4.2 . . . . .	242
4.3	The Integer Factorization Problem . . . . .	243
4.3.1	Older Algorithms . . . . .	244
	Trial division . . . . .	244
	Pollard’s rho method . . . . .	244
	Pollard’s $p - 1$ method . . . . .	245
	Williams’ $p + 1$ method . . . . .	247
4.3.2	The Quadratic Sieve Method . . . . .	248
	The basic algorithm . . . . .	248
	Sieving . . . . .	249
	Incomplete sieving . . . . .	251
	Large prime variation . . . . .	251
	The multiple polynomial quadratic sieve . . . . .	252
	Parallelization . . . . .	253
	TWINKLE: Shamir’s factoring device . . . . .	254
4.3.3	Factorization Using Elliptic Curves . . . . .	255
4.3.4	The Number Field Sieve Method . . . . .	258
	Selecting the polynomial $f(X)$ . . . . .	259
	Construction of $\mathcal{Q}$ . . . . .	259

	Construction of $\mathcal{G}$ . . . . .	259
	Construction of $\mathcal{U}$ . . . . .	260
	Computing the factorization of $a + b\alpha$ . . . . .	260
	Sieving . . . . .	261
	The running time of the SNFSM . . . . .	262
	Exercise Set 4.3 . . . . .	262
4.4	The Finite Field Discrete Logarithm Problem . . . . .	264
4.4.1	Square Root Methods . . . . .	264
	Shanks' baby-step-giant-step method . . . . .	265
	Pollard's rho method . . . . .	265
	The Pohlig-Hellman method . . . . .	266
4.4.2	The Index Calculus Method . . . . .	267
4.4.3	Algorithms for Prime Fields . . . . .	268
	The basic ICM . . . . .	268
	The linear sieve method . . . . .	270
	The number field sieve method . . . . .	272
4.4.4	Algorithms for Fields of Characteristic 2 . . . . .	273
	The basic ICM . . . . .	274
	The adaptation of the linear sieve method . . . . .	275
	Coppersmith's algorithm . . . . .	276
	Exercise Set 4.4 . . . . .	279
4.5	The Elliptic Curve Discrete Logarithm Problem (ECDLP) . . . . .	281
4.5.1	The MOV Reduction . . . . .	282
	The correctness of the algorithm . . . . .	283
	Choosing $k$ . . . . .	284
	Computing $e_m(P, R)$ . . . . .	284
4.5.2	The SmartASS Method . . . . .	286
4.5.3	The Xedni Calculus Method . . . . .	289
	Exercise Set 4.5 . . . . .	291
4.6	The Hyperelliptic Curve Discrete Logarithm Problem . . . . .	292
4.6.1	Choosing the Factor Base . . . . .	293
4.6.2	Checking the Smoothness of a Divisor . . . . .	293
4.6.3	The Algorithm . . . . .	294
4.7	Solving Large Sparse Linear Systems over Finite Rings . . . . .	294
4.7.1	Structured Gaussian Elimination . . . . .	296
4.7.2	The Conjugate Gradient Method . . . . .	297
4.7.3	The Lanczos Method . . . . .	298
4.7.4	The Wiedemann Method . . . . .	299
4.8	The Subset Sum Problem . . . . .	300
4.8.1	The Low-Density Subset Sum Problem . . . . .	301
4.8.2	The Lattice-Basis Reduction Algorithm . . . . .	302
	Exercise Set 4.8 . . . . .	304
<b>5</b>	<b>Cryptographic Algorithms</b> . . . . .	<b>309</b>
5.1	Introduction . . . . .	310
5.2	Secure Transmission of Messages . . . . .	310
5.2.1	The RSA Public-key Encryption Algorithm . . . . .	310
	RSA key pair . . . . .	310
	RSA encryption . . . . .	312

	RSA decryption . . . . .	312
5.2.2	The Rabin Public-key Encryption Algorithm . . . . .	313
	Rabin key pair . . . . .	313
	Rabin encryption . . . . .	314
	Rabin decryption . . . . .	314
5.2.3	The Goldwasser–Micali Encryption Algorithm . . . . .	315
	Goldwasser–Micali key pair . . . . .	315
	Goldwasser–Micali encryption . . . . .	315
	Goldwasser–Micali decryption . . . . .	316
5.2.4	The Blum–Goldwasser Encryption Algorithm . . . . .	317
	Blum–Goldwasser key pair . . . . .	317
	Blum–Goldwasser encryption . . . . .	318
	Blum–Goldwasser decryption . . . . .	318
5.2.5	The ElGamal Public-key Encryption Algorithm . . . . .	319
	ElGamal key pair . . . . .	319
	ElGamal encryption . . . . .	320
	ElGamal decryption . . . . .	320
5.2.6	The Chor–Rivest Public-key Encryption Algorithm . . . . .	321
	Chor–Rivest key pair . . . . .	321
	Chor–Rivest encryption . . . . .	322
	Chor–Rivest decryption . . . . .	322
5.2.7	The XTR Public-key Encryption Algorithm . . . . .	323
	XTR key pair . . . . .	327
	XTR encryption . . . . .	327
	XTR decryption . . . . .	328
5.2.8	The NTRU Public-key Encryption Algorithm . . . . .	328
	NTRU key pair . . . . .	328
	NTRU encryption . . . . .	330
	NTRU decryption . . . . .	331
	Exercise Set 5.2 . . . . .	332
5.3	Key Exchange . . . . .	334
5.3.1	Basic Key-Exchange Protocols . . . . .	334
	The Diffie–Hellman key-exchange protocol . . . . .	334
	Small-subgroup attacks . . . . .	335
	Cofactor exponentiation . . . . .	336
5.3.2	Authenticated Key-Exchange Protocols . . . . .	336
	Unknown key-share attacks . . . . .	336
	The Menezes–Qu–Vanstone key-exchange protocol . . . . .	338
	Exercise Set 5.3 . . . . .	339
5.4	Digital Signatures . . . . .	340
5.4.1	The RSA Digital Signature Algorithm . . . . .	341
5.4.2	The Rabin Digital Signature Algorithm . . . . .	342
5.4.3	The ElGamal Digital Signature Algorithm . . . . .	343
5.4.4	The Schnorr Digital Signature Algorithm . . . . .	344
5.4.5	The Nyberg–Rueppel Digital Signature Algorithm . . . . .	345
5.4.6	The Digital Signature Algorithm (DSA) . . . . .	346
5.4.7	The Elliptic Curve Digital Signature Algorithm (ECDSA) . . . . .	348
5.4.8	The XTR Signature Algorithm . . . . .	349
5.4.9	The NTRUSign Algorithm . . . . .	352

5.4.10	Blind Signature Schemes . . . . .	355
	Chaum's RSA blind signature protocol . . . . .	355
	The Schnorr blind signature protocol . . . . .	356
	The Okamoto–Schnorr blind signature protocol . . . . .	357
5.4.11	Undeniable Signature Schemes . . . . .	357
	The Chaum–Van Antwerpen undeniable signature scheme . . . . .	358
	RSA-based undeniable signature scheme . . . . .	360
5.4.12	Signcryption . . . . .	362
	Exercise Set 5.4 . . . . .	364
5.5	Entity Authentication . . . . .	366
5.5.1	Passwords . . . . .	366
5.5.2	Challenge–Response Algorithms . . . . .	368
	A challenge–response scheme based on encryption–decryption . . . . .	368
	A challenge–response scheme based on digital signatures . . . . .	369
	Mutual authentication . . . . .	370
5.5.3	Zero-Knowledge Protocols . . . . .	370
	The Feige–Fiat–Shamir (FFS) protocol . . . . .	372
	The Guillou–Quisquater (GQ) protocol . . . . .	373
	The Schnorr protocol . . . . .	374
	Exercise Set 5.5 . . . . .	375
<b>6</b>	<b>Standards</b> . . . . .	<b>381</b>
6.1	Introduction . . . . .	382
6.2	IEEE Standards . . . . .	382
6.2.1	The Data Types . . . . .	383
	Bit strings . . . . .	383
	Octet strings . . . . .	383
	Integers . . . . .	384
	Prime finite fields . . . . .	384
	Finite fields of characteristic 2 . . . . .	384
	Extension fields of odd characteristics . . . . .	384
	Elliptic curves . . . . .	385
	Elliptic curve points . . . . .	385
	Convolution polynomial rings . . . . .	386
6.2.2	Conversion Among Data Types . . . . .	386
	Converting bit strings to octet strings (BS2OS) . . . . .	386
	Converting octet strings to bit strings (OS2BS) . . . . .	387
	Converting integers to bit strings (I2BS) . . . . .	388
	Converting bit strings to integers (BS2I) . . . . .	388
	Converting integers to octet strings (I2OS) . . . . .	388
	Converting octet strings to integers (OS2I) . . . . .	389
	Converting field elements to octet strings (FE2OS) . . . . .	389
	Converting octet strings to field elements (OS2FE) . . . . .	389
	Converting field elements to integers (FE2I) . . . . .	389
	Converting elliptic curve points to octet strings (EC2OS) . . . . .	389
	Converting octet strings to elliptic curve points (OS2EC) . . . . .	390
	Converting ring elements to octet strings (RE2OS) . . . . .	390
	Converting octet strings to ring elements (OS2RE) . . . . .	391
	Converting ring elements to bit strings (RE2BS) . . . . .	391

	Converting bit strings to ring elements (BS2RE) . . . . .	391
	Converting binary elements to octet strings (BE2OS) . . . . .	392
	Converting octet strings to binary elements (OS2BE) . . . . .	392
6.3	RSA Standards . . . . .	393
6.3.1	PKCS #1 . . . . .	393
	RSA keys . . . . .	394
	RSA key operations . . . . .	394
	RSAES–OAEP encryption scheme . . . . .	395
	RSASSA–PSS signature scheme with appendix . . . . .	398
	A mask-generation function . . . . .	399
	The RSA encryption scheme of PKCS #1, Version 1.5 . . . . .	400
	The RSA signature scheme of PKCS #1, Version 1.5 . . . . .	401
6.3.2	PKCS #3 . . . . .	402
<b>7</b>	<b>Cryptanalysis in Practice</b> . . . . .	<b>405</b>
7.1	Introduction . . . . .	406
7.2	Side-Channel Attacks . . . . .	407
7.2.1	Timing Attack . . . . .	407
	Details of the attack . . . . .	407
	Countermeasures . . . . .	410
7.2.2	Power Analysis . . . . .	411
	Simple power analysis (SPA) . . . . .	411
	Differential power analysis (DPA) . . . . .	413
	Countermeasures . . . . .	415
7.2.3	Fault Analysis . . . . .	416
	Fault attack on RSA based on CRT . . . . .	417
	Fault attack on RSA without CRT . . . . .	417
	Fault attack on the Rabin digital signature algorithm . . . . .	418
	Fault attack on DSA . . . . .	418
	Fault attack on the ElGamal signature scheme . . . . .	419
	Fault attack on the Feige–Fiat–Shamir identification protocol . . . . .	420
	Countermeasures . . . . .	422
	Exercise Set 7.2 . . . . .	423
7.3	Backdoor Attacks . . . . .	424
7.3.1	Attacks on RSA . . . . .	425
	Hiding prime factor . . . . .	425
	Hiding small private exponent . . . . .	428
	Hiding small public exponent . . . . .	429
7.3.2	An Attack on ElGamal Signatures . . . . .	430
7.3.3	An Attack on ElGamal Encryption . . . . .	431
7.3.4	Countermeasures . . . . .	432
	Exercise Set 7.3 . . . . .	432
<b>8</b>	<b>Quantum Computation and Cryptography</b> . . . . .	<b>437</b>
8.1	Introduction . . . . .	438
8.2	Quantum Computation . . . . .	438
8.2.1	System . . . . .	439
8.2.2	Entanglement . . . . .	440
8.2.3	Evolution . . . . .	442
8.2.4	Measurement . . . . .	443



8.2.5	The Deutsch Algorithm . . . . .	445
	Exercise Set 8.2 . . . . .	446
8.3	Quantum Cryptography . . . . .	448
	Exercise Set 8.3 . . . . .	451
8.4	Quantum Cryptanalysis . . . . .	452
8.4.1	Shor's Algorithm for Computing Period . . . . .	453
8.4.2	Breaking RSA . . . . .	455
8.4.3	Factoring Integers . . . . .	455
8.4.4	Computing Discrete Logarithms . . . . .	456
	Exercise Set 8.4 . . . . .	458

## Appendices

<b>A</b>	<b>Symmetric Techniques</b>	<b>465</b>
A.1	Introduction . . . . .	466
A.2	Block Ciphers . . . . .	466
A.2.1	A Case Study: DES . . . . .	467
	DES key schedule . . . . .	468
	DES encryption . . . . .	468
	DES decryption . . . . .	471
	DES test vectors . . . . .	471
	Cryptanalysis of DES . . . . .	471
A.2.2	The Advanced Standard: AES . . . . .	472
	Data representation . . . . .	472
	AES key schedule . . . . .	473
	AES encryption . . . . .	474
	AES decryption . . . . .	476
	AES test vectors . . . . .	478
	Cryptanalysis of AES . . . . .	478
A.2.3	Multiple Encryption . . . . .	478
A.2.4	Modes of Operation . . . . .	480
	The ECB mode . . . . .	480
	The CBC mode . . . . .	481
	The CFB mode . . . . .	481
	The OFB mode . . . . .	482
	Exercise Set A.2 . . . . .	483
A.3	Stream Ciphers . . . . .	486
A.3.1	Linear Feedback Shift Registers . . . . .	487
A.3.2	Stream Ciphers Based on LFSRs . . . . .	489
	Exercise Set A.3 . . . . .	490
A.4	Hash Functions . . . . .	491
A.4.1	Merkle's Meta Method . . . . .	492
A.4.2	The Secure Hash Algorithm . . . . .	494
	Exercise Set A.4 . . . . .	495
<b>B</b>	<b>Key Exchange in Sensor Networks</b>	<b>497</b>
B.1	Introduction . . . . .	498
B.2	Security Issues in a Sensor Network . . . . .	498
B.3	The Basic Bootstrapping Framework . . . . .	500
B.4	The Basic Random Key Predistribution Scheme . . . . .	502

B.4.1	The $q$ -composite Scheme . . . . .	504
B.4.2	Multi-path Key Reinforcement . . . . .	505
B.5	Random Pairwise Scheme . . . . .	506
B.5.1	Multi-hop Range Extension . . . . .	507
B.6	Polynomial-pool-based Key Predistribution . . . . .	508
B.6.1	Pairwise Key Predistribution . . . . .	509
B.6.2	Grid-based Key Predistribution . . . . .	510
B.7	Matrix-based Key Predistribution . . . . .	511
B.8	Location-aware Key Predistribution . . . . .	513
B.8.1	Closest Pairwise Keys Scheme . . . . .	513
B.8.2	Location-aware Polynomial-pool-based Scheme . . . . .	515
<b>C</b>	<b>Complexity Theory and Cryptography</b>	<b>517</b>
C.1	Introduction . . . . .	518
C.2	Provably Difficult Computational Problems Are not Suitable . . . . .	519
	Exercise Set C.2 . . . . .	519
C.3	One-way Functions and the Complexity Class UP . . . . .	520
	Exercise Set C.3 . . . . .	522
<b>D</b>	<b>Hints to Selected Exercises</b>	<b>523</b>
	<b>References</b>	<b>531</b>
	<b>Index</b>	<b>547</b>